the permutation P* 136 applied after the S boxes 170 to be varied under control of some of the bits

of the cryptographic key 134. The present invention utilizes cryptographic key bits for three

purposes. The first purpose is to furnish the 56 bits (excluding the 8 bits of parity) 138 used to create

the 64 bits (including the 8 bits of parity) 166 that traditional DES uses to compute the elements of

$\beta 1$
$cm old$. the so called key schedule ($118_1...118_{16}$). The second purpose is to supply cryptographic key bits

142 that are used to control the generation and replacement of the variable P* permutation 136. The

third purpose is to provide a privacy means 150 such that encipherment of a data block 110 and

decipherment of a cipher block 132 can be accomplished in private by using a secret mask 150 which

determines which subset of cryptographic key bits 138 selected from the cryptographic key 134 are

used for the DES key schedule 168 and which subset of the remaining cryptographic key bits 142

are used for the control and generation of the variable P* permutation 136.

Please AMEND the second paragraph beginning on page 13, line 10 to read as follows:

The steps for carrying out data encryption using the enhanced DES method according to the

present invention is shown in Fig. 1. An input data block of 64 bits in step 110 is subjected to an

initial permutation 112. The initial permutation in step 112 provides no cryptographic benefit but

$\beta 2$
$Cm t$ ensures compatibility with other implementations. That is, the initial permutation simply transposes

bits within the input block in accordance with a table given in the conventional DES. The initially

permutated data are then divided into a left half register block (L_0) 114 and a right half register block

(R_0) 116 of 32-bits each. The right half register block 116 and K_1 118_1 a derivative of super keying

variable (SK $_K$) 134 are used as inputs to the f function 120 whose output 176 is bit-by-bit modulo-2

2

added 122 with the left half register block L_0 114 . The K_n 118_n in the formula below is generated according to the DES key schedule 168 shown in Fig. 8.

Please AMEND the second paragraph beginning on page 14, line 4 to read as follows:

The output at the end of 16 rounds consists of a preoutput which is the concatenation of R_{16} 126 and L_{16} 128. Subsequently, after an inverse initial permutation in step 130, an output block of 64 bits 132 is produced.

Please AMEND the third paragraph beginning on page 14, line 7 to read as follows:

Fig. 2 shows an example of utilizing super keying variable (SK) 134 of K bits in length. In an example in which K= 128 bits, a mask 150 selects 56 bits 138 which needs to be expanded to 64 bits with odd parity 166 for the DES key schedule 168 of Fig. 8 while the remaining K-56 bits 142 are used for P* programming. In particular, Fig. 2 shows that the remaining K-56 bits 142 are selected for programming e.g., an M-sequence linear feedback shift register (LFSR) 144 which in turn supplies, under the control of a control module 200, bits to be used as beta-elements 182(See Fig. 4) in the Field Programmable Gate Array FPGA 136 which in turn implements the P* permutation 136. The f function 120 contains the S boxes 170 which produce a 32 bit output labeled (B1,B2, ...,B32) 148. These 32 bits are transposed by the P* permutation 136 resulting in a one-to-one transposition labeled (B1*,B2*,...,B32*) 174.

Please AMEND the fourth paragraph beginning on page 14, line 17 to read as follows:

The 32 bits 174 resulting from application of P* are further permuted by a fixed one-to-one permutation P' 184 resulting in 32 output bits 176. The P' permutation would normally be calculated at the time of designing the embodiment and is calculated so that when the beta elements of the FPGA 136 are all set to a particular default condition, which in our preferred embodiment is all zeros, the fixed P' permutation 184 is such that equivalent to the fixed and defined P permutation of the traditional DES. This is the feature that enables the present invention to have a mode that is compatible with the traditional DES. Note that the above referenced P permutation is identified in U.S. Patent No.: 3962539 as 600 and its values are specified on page 15 of FIPS 46-3 as permutation function P.

Please AMEND the first paragraph beginning on page 15, line 8 to read as follows:

The operation of the process needed to select from the SuperKey 134 the DES engine sub key 138 and the subkey 142 used to generate and or replace P* is controlled by a control module 200. This module may also be used to control bits from a randomizer 208 when the system is in the mode of generating non-reproducible and non-predictable output (i.e. unable to be decrypted or replicated by another party with the same device and settings) for use such as in generating cryptographic keys or wherever non deterministic or difficult to predict information is required.

Please replace the second paragraph beginning on page 15, line 15 to read as follows:

B7

The following is an example of an application of the privacy feature of the preferred embodiment of the present invention. Two users of an instant messaging application over the internet each have an identical implementation of the applicants' improved invention. A cipher key (e.g. 128 bits)134 is securely supplied to each user by the messaging system. This enables the users to encrypt and decrypt messages to each other using the identical cipher key. However, depending upon the architecture and implementation of the cipher key generation and distribution system the messaging system operator may be able to hold a copy of the cipher key134 allowing unauthorized reading of the messages sent between users. The users may wish to achieve additional privacy to protect against this unauthorized reading of messages. This can be accomplished using the present invention as follows.

Please replace the first paragraph beginning on page 16, line 3 to read as follows:

B8
Cont

First the users agree upon a secondary cipher key using an independent channel from that of the messaging service. This secondary cipher key could be another 128 bit cipher key or a mutually agreed upon pass phrase of enough length that it can be converted by a means such as ASCII representation into a binary mask 150 of 56 ones which is used to select 56 bits of sub key 138 from the original cipher key 134. The bits in the original cipher key positions corresponding to the positions of the 56 ones in the mask become the ordered 56 bits of the sub key 138. The remaining ordered 72 bits of the original cipher key are used to preset a portion of an M sequence LFSR 144

5

which generates bits for changing P*. The result is that the two users now have used the identical

initial cipher key but each has modified it in the same unique way. This modification is as secure

as the independent channel used to communicate the secondary cipher key and the means of selecting

the secondary cipher key or pass phrase. If this secondary cipher key is in fact securely

communicated between the two users then the users are protected against the possibility of the

messaging service operator using a copy of the original cipher key in an unauthorized manner to read

the messages between the two users. The situation of the messaging service operator providing

pathological cipher keys such as all zeros or all ones can be checked for by the users' application.

Please replace the second paragraph beginning on page 16, line 19 to read as follows:

The heart of the cryptosecurity of the applicants' improved DES system resides in the f

function 120 as shown in Fig. 3. As shown in Fig. 3, the register block (R) 116 is expanded by E

158 to 48 bits by repeating certain bits of the register block. This expansion is defined by a table E

in the conventional DES. The 48-bit expanded register block 162 is then bit-by-bit modulo-2 added

164 with the nth element K_n of the key schedule 168 which is derived from the expanded 64 bit sub

key 166 which in turn is derived from the 56 bits 138 selected using the mask 150 from the super

keying variable (SK) 134 of 128 bits. The result of this operation is passed to a substitution step 170.

The selection step 170 is made up of eight unique substitution functions. Each of the unique

substitution functions (i.e., S-boxes designated as $S_1,...,S_8$) takes a 6-bit block as input and yields

a 4-bit block as output. The operation of each of the eight S-boxes is defined by the conventional

DES.

Please replace the second paragraph beginning on page 17, line 12 to read as follows:

The dynamic permutation process (DPP) 136 using a five-stage Omega Network is shown in Fig. 4. The Omega network is based on a plurality of Beta switch elements 182, each of which has two inputs and two outputs and a one bit control. Contrary to the conventional DES permutation process in which the P permutation applied after the S boxes is fixed and known, the permutation results of the DPP are dependent upon the particular Beta (*) values as set forth in each of the Beta switch elements. Some or all of the Beta values are not known because they can be supplied by the cryptographic key or cryptovariable.

Please replace the third paragraph beginning on page 18, line 16 to read as follows:

Fig. 6 illustrates the Omega Network as shown in Fig. 5 combined with the related fixed permutation 184 of 32 elements. That is, by cascading the Omega network with the appropriate P' permutation 184, the combination of the DPP followed by P' yields a permutation that corresponds to the original P function in the traditional DES. The permutation mapping of the P' function which is defined in Table 1 is the fixed permutation which when applied after a P* produced by the Omega network with Beta elements set to the default condition zero yields the P permutation of the traditional DES.

Please replace the first paragraph beginning on page 20, line 3 to read as follows:

B12

For each round of the encryption process, the permutation in each f function can be varied, and the variation need not by cyclic after sixteen rounds but non-repeating throughout an encryption. Additionally, the variation in the permutation can also be a function of the extended keying variable.

Please replace the third paragraph beginning on page 20, line 15 to read as follows:

B13

Since the Omega network as shown in Fig. 6 requires 80 one bit controls, some of these controls can be set by utilizing bits from the cryptographic key that are not used in the calculation of the key schedule, i.e. that are not used in 138. These control bits from the keying variable would then be invariant over the life of that particular keying variable. The remaining controls would be fixed or be a function of the round of the ECB mode and a function of the round number plus. In the k-bit cipher feedback mode, the encipherment cycle number would be zero for the production of the first k-bits, one for the production of the second k-bits, and so on. Thus the round number plus 16 times the encipherment cycle number would be 1, 2, 3, ..., 16, 17, 18, ..., 31, 32, respectively, for the 32 rounds involved in the production of the first two k-bit blocks. It may also be that the bits for the Beta elements be a function not only of the round number plus 16 times the encipherment cycle number, but also the Initialization Vector (IV) which in the Output Feedback mode would be 110.

8

Please replace the first paragraph beginning on page 21, line 5 to read as follows:

β14

The number of bits from the cryptographic keying variable, and the number of bits from the sources described above, would need to sum to 80 as this is the number of one-bit controls needed to set the 5 level 32 input omega network. A standard key length is 128 bits, so in the present invention a preferred embodiment would use 56 bits for the traditional DES key schedule and the remaining 72 bits as control bits for 72 Beta elements. The additional 8 bits needed to completely define the 80 element omega network in this example could be fixed for a particular implementation or use or could be variable within a cryptoperiod or from cryptoperiod to cryptoperiod.

Please replace the third paragraph beginning on page 23, line 15 to read as follows:

β15

Additionally, a network referred to as the Benes-Waksman network, which is realizable with Beta elements for all of the 32! permutations, can also be used in the present invention as an alternative arrangement for the permutation network. The Benes-Waksman network differs from the Omega network in the sense that every stage is not identical in its connection to every other stage. However, it is also understandably more complex than the omega network considered above.